REMARKS/ARGUMENTS

The Office Action mailed October 23, 2003 has been reviewed and carefully considered. Claims 1, 3, 10, 17, 18, 19, and 22 are amended. Claims 1-26 are pending in this application, with claim 1 being the only independent claim. Reconsideration of the above-identified application, as herein amended and in view of the following remarks, is respectfully requested.

In the Office Action mailed October 23, 2003, the drawings are objected to by the draftsperson as containing minor informalities. Attached hereto are a set of formal drawings for the present application which address the draftspersons concerns. Accordingly, the drawings should now be accepted.

Claims 3-4 and 19 stand rejected under 35 U.S.C. §112, second paragraph, as being indefinite because they contain the phrase "or the like". The listing of the claims listed above starting on page 2 of this document represent the claims applicant has on file as being submitted to the U.S. Patent and Trademark Office. Claims 3, 4 and 19 do not recite the phrase "or the like". Accordingly, it is respectfully requested that the rejection of claims 3, 4, and 19, under 35 U.S.C. §112, second paragraph, now be withdrawn.

Claims 1-26 stand rejected under 35 U.S.C. §102(e) as anticipated by U.S. Patent No. 6,367,013 (Bisbee).

Before discussing the cited prior art and the Examiner's rejections of the claims in view of that art, a brief summary of the present invention is appropriate. The present invention relates to a method for using a previously certified identity to create another representational form for the same identity (page 4, lines 34-36 of the present application). According to a specific embodiment, applicant's system is used to securely sign a PGP key by Wireless Public Key

Infrastructure (WPKI) using the applicant's SIM card to link the signature back to the proof of identity that was provided to the WPKI Local Registration Authority (LAR) (page 8, lines 30-35).

According to the embodiment, software on a PC communicates with a phone of the user containing the SIM card and sends a message to start the PGP signing procedure (page 9, lines 17-20). The phone generates and displays a four digit random number which must be entered into the PC (page 9, lines 25-27). The software on the PC sends a first message to the phone including the number which requests a certificate authority (CA) to lookup a user ID for the phone network identification (page 9, line 35 to page 10, line 3). The phone signs the first message if the numbers match and the message is returned to the PC where it is stored for future transmission to the CA (page 10, lines 8-15). The above steps describe the creation of a request for a second electronic identity, as recited in step (b) of claim 1.

The PC software sends a second message to the phone requesting it to sign the attached key (page 10, lines 15-23). The user verifies that the PGP fingerprint on the phone is the same as that on the PC and signs using the phone and send the second message back to the PC (page 10, lines 24-33). The phone connection to the PC is no longer needed. The second message is the message to be sent in step (h) of claim 1.

The PC then contacts the CA and sends the request for User ID, i.e., the first message, to the CA (page 11, lines 7-10) (step (c) of claim 1). The CA looks up the user ID of the phone's owner and sends it back to the PC, the user ID being the WPKI User ID that the phone owner certified at the Local Registration Authority (page 11, lines 11-14) (steps (d)-(f) of claim 1).

The PC next sends the second message which was signed by the phone to the CA (page 12, lines 7-10) (steps (g) and (h) of claim 1). The CA checks the PGP signature, the phone key, and the user ID (the ID of the phone) which signed the second message (page 12, lines 13-16) (step (i) of claim 1). If the key is in the CA database, the second identity is issued to the user (step (j) of claim 1).

Independent claim 1, and dependent claims 3, 10, 17, 18, 19, and 22, are amended to correct minor typographical errors and to correct antecedent basis in the claims.

Independent claim 1 is drawn to a method for issuing an electronic identity for a first entity from an identity registration authority, and recites the steps "creating a request for a second electronic identity for said first entity, the request including an identifier of said first entity", after sending the request to an identity registration authority and receiving an identification response from the identity registration authority, "verifying an acceptability of said identification response by said first entity", "signing digitally said identification response by said first entity" if the identification response is acceptable, "sending said signed response to said identity registration authority", and "issuing a second identity based on said first identity" if said digital signature and identification response are valid.

Bisbee fails to disclose the present invention because (1) Bisbee does not disclose issuing an electronic identity for identifying an entity and (2) Bisbee does not disclose issuing a second electronic identity for an entity based on a first electronic identity of the entity.

Regarding the first reason, Bisbee relates to document authentication system and methods for providing a verifiable chain of evidence and security for the transfer and retrieval of <u>documents</u> and other information objects in digital format (col. 1, lines 16-19 and lines 33-34; col. 6, lines 66 in Bisbee). As stated in the abstract of Bisbee, digital signatures are not valid indefinitely but only during validity periods of the authentication certificates. Bisbee further states that electronic original objects are created by signing information objects by a transfer agent (col. 4, lines 33-36; see also col. 10, lines 33-36 for a definition of e-original object and e-original). Accordingly, the signatures on the e-original objects of Bisbee are created by the entities recited in the present invention.

In contrast to the present invention, Bisbee relates to lengthening the validity periods of digital signatures for electronic information objects (col. 13, lines 7-12). Accordingly, Bisbee fails to disclose the step of "creating a request for a second electronic identity for said first entity" and " issuing a second identity", as expressly recited in independent claim 1. The Examiner states that col. 5, lines 6-35 disclose the step of issuing a second identity. However, this section refers to a method of handling stored e-original objects and stamping each validated e-original. It is respectfully submitted that this has nothing to do with issuing identities of entities.

Claim 1 also recites that the entity for which the second identity is being issued performs the following steps: "verifying an acceptability of said identification response by said first entity" after sending the request to an identity registration authority and receiving an identification response from the identity registration authority, and "signing digitally said identification response by said first entity" if the identification response is acceptable. In Bisbee, the e-original document whose validation is being extended can not itself perform these steps because it is a document. Rather the validations are performed by third parties in Bisbee because the document itself can not, by definition, perform any steps. Accordingly, it is respectfully submitted that Bisbee fails to disclose issuing a second electronic identity for said first entity, as recited in independent claim 1.

Furthermore, Bisbee also fails to teach or suggest issuing a second identity for an entity based on a first identity of the entity. In contrast, Bisbee discloses lengthening validity periods of digital signatures for electronic information objects. Col. 5, lines 6-35 of Bisbee, cited by the Examiner, discloses that a second trusted custodial utility can apply a digital signature and authentication certificate to the document. However, Bisbee fails to disclose issuing a second identity for the electronic document.

In view of the above remarks, it is respectfully submitted that independent claim 1 is not anticipated by Bisbee under 35 U.S.C. §102.

Furthermore, since Bisbee relates to lengthening validity periods for electronic original documents, Bisbee fails to teach or suggest issuing a second electronic identity for an entity based on a first electronic identity of the entity. Accordingly, it is respectfully submitted that independent claim 1 is also allowable over Bisbee under 35 U.S.C. §103.

Dependent claims 2-26, being dependent on independent claim 1, are deemed allowable for the same reasons expressed above with respect to independent claim 1.

The application is now deemed to be in condition for allowance and notice to that effect is solicited.

It is believed that no fees or charges are required at this time in connection with the present application; however, if any fees or charges are required at this time, they may be charged to our Patent and Trademark Office Deposit Account No. 03-2412.

Respectfully submitted,

COHEN, PONTANI, LIEBERMAN & PAVANE

By Alfred W. Froebrich

Alfred W. Froebrich
Reg. No. 38,887
551 Fifth Avenue, Suite 1210
New York, New York 10176
(212) 687-2770

Dated: January 23, 2004